## REMARKS

### INTRODUCTION

Claims 1-26 were previously pending and under consideration.

Claims 1-26 are cancelled herein.

Claims 27-44 are added herein.

Therefore, claims 27-44 are now pending and under consideration.

No new matter is being presented, and approval and entry are respectfully requested.

### REJECTIONS UNDER 35 USC § 103

In the Office Action, at pages 2-3, claims 1, 6, 11, and 24-26 were rejected under 35 U.S.C. § 103 as being unpatentable over Schlafly in view of Rosenthal. Claims 2-5 and 7-10 were rejected under 35 U.S.C. § 103 as being unpatentable over Schlafly in view of Rosenthal and further in view of Dolan. Claims 4 and 9 were rejected under 35 U.S.C. § 103 as being unpatentable over Schlafly in view of Rosenthal, in view of Dolan and further in view of Bellare. These rejections are traversed and reconsideration is requested.

Claim 27, for example, recites information being divided into data divisions. Authenticators specific to data divisions are generated by different one-way functions with different keys, and the authenticators are appended to the information so that both are sent to a certifier. Each authenticator specific to a data division is generated by applying to the data division a respective different one-way function using a different key. For any given input information that is divided, a data division thereof is processed by its respective one-way function; different data divisions have authenticators produced in different manners.

The rejection cites Rosenthal as teaching the use of different one-way functions. The rejection states that "Rosenthal discloses using a variety of different checksum calculation methods" to provide Schlafly's lack of "a different one-way hash function on each of the divided data". Rosenthal is inapplicable to the present claims because its checksum/CRC calculations do not produce a different appended authenticator specific to a division of input information. The checksum and CRC in Rosenthal are single values for the entire program (information).

The checksum is calculated by summing all of the bytes of the original program, and the CRC is calculated by XOR'ing all of the bytes of the original program (col. 9, lines 23-28). Although Rosenthal does discuss variant methods, these variant methods all concern finding a single checksum and a single CRC for the entire input information (program). Rosenthal does not have a first checksum variant (first function) calculating a checksum (first authenticator) specific to one division of the program (information) and another variant calculating a checksum (second authenticator) specific to another division of the program. Rosenthal uses two different functions to calculate two different authenticators on the entire information. Different authenticators calculated with different functions of different respective divisions are not discussed or suggested. In other words, the Bytes/divisions of Rosenthal do not have authenticators specific thereto.

In the prior art, when using a one-way function, security was enhanced by increasing the size of blocks processed by a single one-way function. However, this required rigorous verification of the properties of the one-way function and other difficulties that occur. No prior art discusses or suggests that the usefulness of authenticating with one-way functions can be improved by dividing input information into divisions and using different one-way functions, with different keys, to come up with different respective authenticators for the divisions. See the first two paragraphs on page 3 of the specification.

Withdrawal of the rejection is respectfully requested.

**DEPENDENT CLAIMS**

The dependent claims are deemed patentable due at least to their dependence from allowable independent claims. These claims are also patentable due to their recitation of independently distinguishing features. For example, claim 3 recites that the appending unit appends authenticators obtained by truncating the first and second authenticators to the information. This feature is not taught or suggested by the prior art. Withdrawal of the rejection of the dependent claims is respectfully requested.

**CONCLUSION**

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 7 Oct 2004

By: James Strom

James T. Strom
Registration No. 48,702

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501